

An International Cyber Warfare Treaty: Historical Analogies and Future Prospects

Alexi Franklin

INTRODUCTION

The earliest philosophical thinking on what we now call the Just War tradition began in ancient Rome with Augustine of Hippo.¹ While the theory has grown to incorporate new concepts and been refined in the millennium and a half since his passing, its underlying core concept—that circumscribed warfare can be conducted in a righteous, morally upright manner—remains.² At best, these precepts are unevenly upheld, but they persist as an ideal that has proliferated to become a generally accepted concept worldwide.

In the twentieth and twenty-first centuries, the latest refinements to the Just War theory have focused on specific classes or subclasses of weapons—such as landmines, cluster munitions, and chemical, biological, and nuclear weapons—thought to be so inhumane, indiscriminate, and uncontrollable as to merit their prohibition.³ Various functional treaties have been attempted to this effect, such as the 1972 Anti-Ballistic Missile Treaty⁴ and the 1987 Intermediate-Range Nuclear Forces Treaty.⁵ These bilateral treaties have sought to curb the mere development of otherwise permissible

¹ Judith Gail Gardam, *Proportionality and Force in International Law*, 87 AM. J. INT'L L. 391, 394–97 (1993).

² See *id.* at 397–99.

³ See *id.*; Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 AM. J. INT'L L. 715, 723–25 (2008) (“Such specific prohibitions of weapons follow a realization that some weapons, by their nature, are likely to inflict greater injuries . . . than is actually warranted by those weapons’ strategic effectiveness.”).

⁴ Limitation of Anti-Ballistic Systems, U.S.-U.S.S.R., May 26, 1972, 23 U.S.T. 3435.

⁵ Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate-Range and Shorter-Range Missiles, U.S.-U.S.S.R., Dec. 8, 1987, 1657 U.N.T.S. 2.

weapons technologies in ways which are thought to make the prospect of general war less likely.

Today, cyber warfare regularly stretches the bounds of acceptable behavior *vis-à-vis* international law. Russia's 2007 cyberattacks on Estonian networks was disruptive but, generally speaking, not dangerous.⁶ Similarly, the United States' 2010 cyber sabotage of Iran's nuclear weapons program via the Stuxnet intrusion, while novel, does not seem to upend fundamental concepts of international law.⁷

By contrast, the alleged 2015 attack by Russia, which disabled the Ukrainian power grid in the dead of winter, was an act carrying the potential to produce fatal consequences for countless civilians.⁸ Cyberattacks of this nature can easily be considered blatant breaches of international law. Thus, continued, unbounded cyber warfare has the potential to render significant consequences for civilians across the globe. Efforts must be made to curb such conduct, both to protect noncombatants from serious collateral damage and to prevent cyber conflicts from escalating into kinetic ones.

Cyber warfare weapons occupy a new class of offensive warfighting weapons whose effects can philosophically and realistically encompass much of the same conduct addressed by core international humanitarian law treaties. Arguably, cyber weapons are legally and (more importantly) tacitly operating outside of existing treaty law. There have been nascent attempts to enact bilateral cyber *détentes*, and there have been attempts to reconcile cyber warfare with existing treaty law. Ultimately these attempts are stumbling towards the

⁶ See Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 16, 2007, 11:32 PM), <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

⁷ See Kim Zetter, *Legal Experts: Stuxnet Attack on Iran was Illegal 'Act of Force'*, WIRED (Mar. 25, 2013, 12:53 PM), <https://www.wired.com/2013/03/stuxnet-act-of-force> (expressing how experts considered the cyberattack an "act of force," but at the same time remained uncertain whether it constituted an "armed attack, which would entitle Iran to use counterforce in self-defense").

⁸ See Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid> ("Whatever the intent, it was a first-of-its-kind attack that set an ominous precedent for the safety and security of power grids everywhere.").

same goal: to bring cyber warfare into the existing constellation of international law. By looking at analogous technological weapons, their respective treaties, and early efforts to craft cyber warfare agreements, this Article seeks to uncover the best-suited, analogous niche that cyber warfare fits into, with regard to successful extant treaty law. Likewise, this Article aims to determine which (if any) treaties would provide the best model to combat and control cyber warfare in the future.

While an international legal cyber framework has yet to be agreed upon, many of the current treaties and agreements under international law arguably apply to the cyber realm. But as of yet, they do not explicitly do so.⁹ Despite this, the majority of existing international treaties could include a range of potential cyber warfare activities without rethinking the underlying Just War principles on which they are based. However, unless such conduct is expressly delineated and agreed upon, nation-states will continue to exceed any implied limitations until they become explicit.

I. ANALOGOUS TECHNOLOGIES AND TREATIES

The timeline for enacting a treaty is long, and adherence by member states typically uneven. For example, the first documented use of chlorine gas in armed conflict occurred in 1915 during World War I. Yet it took a decade for the League of Nations to adopt the Geneva Protocol,¹⁰ and even longer for its parties to enter it into the force of law.¹¹ Over eighty years later in 1997, the Chemical Weapons Convention went into force with controls to enact an outright ban of the “development, production, stockpiling and use” of chemical

⁹ See, e.g., U.N. TREATY COLLECTION, <https://treaties.un.org/Pages/Home.aspx?lang=en>; *Treaties & Agreements*, ARMS CONTROL ASS'N, <https://www.armscontrol.org/treaties>.

¹⁰ Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65 [hereinafter Geneva Protocol].

¹¹ See *id.* at 67, 69, 71; see also U.S. DEP'T OF STATE, TREATIES IN FORCE 497 (2018), <https://www.state.gov/documents/organization/282222.pdf> (noting that the Geneva Protocol entered into force February 8, 1928, but not for the United States until April 10, 1975”).

weapons,¹² a taboo the world has seen broken as recently as a few months ago.¹³ Nevertheless, implementation of the CWC has led to the elimination of many nations' chemical weapons programs and chemical weapons stockpiles, which is an unequivocal global good. Thus, while treaties may not always lead to perfect outcomes, they can still be significant contributors to achieving global peace and safety.

A. Biological Weapons and the Biological Weapons Convention

To a great degree, biological weapons are taxonomically similar to cyber weapons. They can almost spread organically from one host to another, and the initial introduction to its host is intended to be discreet in nature. The consequences of biological weapons can also vary widely, from the irritating to the fatal. For both cyber weapons and biological ones, a central goal is not to eliminate one's opponent, but instead, to incapacitate them. Both weapons are insidious, unseen agents whose spread is unknowable and uncontrollable, but for which there is a potential pre-event prophylaxis as well as a post-event reconstitution. In theory, a strain of a cyber weapon or biological agent, once proliferated, could be isolated and turned back against ones' opponent. Moreover, attribution of either weapon can be difficult, if not impossible.

The Biological Weapons Convention (BWC) is one of the most widely ratified treaties in the world, with 182 state-parties.¹⁴ However,

¹² Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, S. Treaty Doc. No. 103-21, 32 I.L.M. 800 [hereinafter Chemical Weapons Convention]; TREATIES IN FORCE, *supra* note 11, at 498 ("Entered into force April 29, 1997; for the United States May 25, 1997.").

¹³ See Michael D. Shear et al., *U.S. Has Seen Chemical Weapons Activity in Syria, Pentagon Says*, N.Y. TIMES (June 27, 2017), <https://www.nytimes.com/2017/06/27/world/middleeast/syria-chemical-attack-trump.html>.

¹⁴ Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163 [hereinafter Biological Weapons Convention]; see Daryl Kimball, *The Biological Weapons Convention (BWC) at a Glance*, ARMS CONTROL ASS'N, <https://www.armscontrol.org/factsheets/bwc> (last updated Sept. 26, 2018).

despite repeated attempts, the BWC still lacks any verification mechanisms.¹⁵ The BWC is simultaneously vague and all-inclusive as to what materials are prohibited, with Article I of the treaty proscribing all “[m]icrobial or other biological agents, or toxins whatever their origin or method of production.”¹⁶ But it also permits for the production of small quantities of biological agents for “prophylactic, protective or other peaceful purposes.”¹⁷

The broad and open-to-interpretation nature of the BWC is a good fit for a potential cyber treaty, as cyber warfare also involves an ever changing, ever evolving scientific landscape. However, there are still some caveats which do not portend well for a BWC-style cyber treaty. The lack of a verification mechanism in the BWC is owed to the near impossibility of its implementation, given the dual-use nature of many biological weapons’ production methods. Private companies working in the biological sciences harbor grave reservations about BWC verification due to the hypothetical possibility of intrusive treaty inspections facilitating industrial espionage.¹⁸ Cyber-related organizations would be similarly reticent to participate in any verification regime.

In sum, it is impossible to claim the BWC has succeeded; at best, it has not failed. Biological weapons were never used in modern, state-on-state warfare in the decades preceding the BWC’s ratification in 1975. Thus, the Convention was merely a confirmation of the taboo, not the originator of it. Moreover, while biological weapons may be analogous with some aspects of cyber weapons, by and large, biological weapons and the BWC’s model in particular are not a good match for a potential cyber warfare treaty.

¹⁵ See, e.g., Laura H. Kahn, *The Biological Weapons Convention: Proceeding Without a Verification Protocol*, BULL. ATOMIC SCIENTISTS (May 9, 2011), <https://thebulletin.org/biological-weapons-convention-proceeding-without-verification-protocol>; see also *Biological Weapons*, U.N. OFF. FOR DISARMAMENT AFF., <https://www.un.org/disarmament/wmd/bio> (detailing the decades-long, unsuccessful attempts at negotiating and developing a verification regime “to further strengthen the BWC”).

¹⁶ Biological Weapons Convention, *supra* note 14, at 166.

¹⁷ *Id.*

¹⁸ See Gert G. Harigel, *Introduction to Chemical and Biological Weapons*, CARNEGIE ENDOW. FOR INT’L PEACE (Jan. 18, 2001), <http://carnegieendowment.org/2001/01/18/introduction-to-chemical-and-biological-weapons-pub-630>.

B. Chemical Weapons and the Chemical Weapons Convention

Despite most common comparisons to biological or nuclear weapons, cyber weapons also bear many similarities to chemical weapons. Arguably, cyber weapons are conceptually more similar to chemical weapons in their makeup than biological ones. Rather than a logical, discrete combination of elements on the periodic table of the elements, cyber weapons are logical, discrete combinations of computing code. They do not require extensive laboratory training, equipment, or aseptic conditions to construct. In many instances, simple off-the-shelf solutions will suffice. The barrier for technical entry can be low, even down to the level of the at-home hobbyist. Multiple actors have employed them on multiple occasions, with potential outcomes varying from the merely irritating to the fatal.

The Chemical Weapons Convention (CWC) has been committed to by every member state of the United Nations, with 193 state-parties.¹⁹ In contrast to the BWC, the CWC has an intergovernmental implementing body, the Organization for the Prohibition of Chemical Weapons, with on-site verification authority.²⁰ The treaty is extremely particular, with specific chemicals listed by different “schedules” with forty-three specific molecules that have varying levels of control and restriction.²¹

Yet, the highly specific schedule scheme of the CWC makes it a poor fit for any comparison to a potential cyber treaty. There are currently 118 known elements on the periodic table, and the number of

¹⁹ Chemical Weapons Convention, *supra* note 12; *Evolution of the Status of Participation in the Convention*, ORG. FOR THE PROHIB. OF CHEM. WEAPONS, <https://www.opcw.org/evolution-status-participation-convention> (last updated June 16, 2018).

²⁰ Chemical Weapons Convention, *supra* note 12, art. 8; *see Preventing the Re-Emergence of Chemical Weapons: Verification*, ORG. FOR THE PROHIB. OF CHEM. WEAPONS, <https://www.opcw.org/our-work/preventing-re-emergence-chemical-weapons>.

²¹ *See* Chemical Weapons Convention, *supra* note 12, at 265–66; Peter Boehme, *The Verification Regime of the Chemical Weapons Convention: An Overview*, ORG. FOR THE PROHIB. OF CHEM. WEAPONS (Nov. 28, 2008), <https://www.opcw.org/media-centre/news/2008/11/verification-regime-chemical-weapons-convention-overview>.

useful, stable elements is significantly smaller. Consequently, the number of combinations for producing chemical agents is necessarily finite. While there will always be room for additional development and refinement of chemical weapons, they possess inherent limits which are not applicable for to cyber weapons.²² The CWC entered into force in 1997, long after the widespread use of chemical weapons. Hence, the Convention seems to have led to a significant reduction in the production, stockpiling, and employment of chemical weapons following its ratification, which is a positive sign for the feasibility of a similarly suited cyber weapons convention. The establishment of a governing body to oversee the CWC's implementation is of potential intrigue for a theoretical cyber treaty, but the intrusive, on-site verification regime is almost certain to be infeasible, due to the abstract and intangible, digital nature of cyber weapons.

C. The Nuclear Non-Proliferation Treaty

There are many similarities between nuclear and cyber weapons. Only the most technically competent nations are significant cyber powerhouses, and the overlap between nuclear capabilities and cyber power is almost absolute. In fact, the deterrence model of mutually assured destruction seems to be holding the worst possible cyber conflicts at bay. Moreover, the vast majority of the public lacks a working understanding of the technical aspects of either weapon, which makes their existence even more terrifying. The most significant difference between cyber and nuclear weapons is the massive death and destruction that can be wrought by the employment of just a single nuclear weapon. The scale of such destruction is orders of magnitude greater than the consequences of even the most effective cyber weapons.²³

²² See generally Philip Ball, *How Many More Chemical Elements Are There for Us to Find?* BBC EARTH (Jan. 15, 2016), <http://www.bbc.com/earth/story/20160115-how-many-more-chemical-elements-are-there-for-us-to-find>.

²³ See Patrick Cirenza, *The Flawed Analogy Between Nuclear and Cyber Deterrence*, BULL. ATOMIC SCIENTISTS (Feb. 22, 2016), <https://thebulletin.org/2016/02/the-flawed-analogy-between-nuclear-and-cyber-deterrence>.

All but five nations have joined the Nuclear Non-Proliferation Treaty (NPT).²⁴ The International Atomic Energy Agency (IAEA), an independent intergovernmental organization that predates the NPT,²⁵ was accorded with robust and intrusive, on-site verification authority to oversee compliance.²⁶ The NPT is simultaneously vague and all-inclusive, prohibiting the transfer, assistance, or manufacture of “nuclear weapons or other nuclear explosive devices” from nuclear to non-nuclear states.²⁷ Similar to the BWC, the NPT allows states to “develop research, production and use of nuclear energy for peaceful purposes.”²⁸

As discussed previously, robust, on-site verification is a bad fit for cyber weapons. States would likely be unwilling to forego offensive cyber tools in such a sweeping manner as proposed by the NPT. In contrast to both the BWC and the CWC, the NPT has had a number of high-profile failures, most notably with North Korea’s withdrawal and subsequent production of nuclear weapons. Syria, Libya, and Iraq have all possessed nascent nuclear weapons despite their NPT membership and IAEA inspections. Meanwhile, Iran’s shadow nuclear enterprise further complicates the sanctity of the NPT.

Less overt, but more pernicious, is the lack of definitive disarmament on the part of nuclear weapon states despite their treaty obligations. The NPT calls for the ultimate disarmament of all nuclear weapon powers. Although massive, post-Cold War nuclear weapon stockpile reductions did occur, no contemporary nuclear powers have any active plans to eliminate their nuclear weapons programs. As long as nuclear weapons remain useful for deterrence, it is likely they will remain in existence. States will continue to covet them, and the slow proliferation of these weapons across the globe may continue. Much of

²⁴ Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161 [hereinafter Non-Proliferation Treaty]; see *Treaty on the Non-Proliferation of Nuclear Weapons (NPT)*, U.N. OFF. FOR DISARMAMENT AFF., <https://www.un.org/disarmament/wmd/nuclear/npt> (stating a “total of 191 States have joined the Treaty”).

²⁵ See Statute of the International Atomic Energy Agency, July 29, 1957, 8 U.S.T. 1093, 276 U.N.T.S. 3; see also *Statute*, IAEA, <https://www.iaea.org/about/overview/history> (unanimously approved by eighty-one nations in October 1956).

²⁶ See Non-Proliferation Treaty, *supra* note 24, arts. 3, 8.

²⁷ *Id.* art. 1.

²⁸ *Id.* art. 4.

the same could be said of cyber weapons. As a result, the NPT is also likely not an ideal model for duplication in the cyber realm.

D. The Mine Ban Treaty and Convention on Cluster Munitions

Moving beyond the banning of entire classes of weapon technologies, an example for regulating specific types of weapons might be a more apt approach to cyber weapons. Non-nuclear explosive weapons are still globally permissible for use in warfare, but specific types of such weapons have been partially banned—specifically landmines and cluster munitions.

The Anti-Personnel Mine Ban Convention (or Mine Ban Treaty) is conceptually flawed, as it still enables the employment of vehicle mines.²⁹ Anti-vehicle mines often result in civilian fatalities by virtue of destroying a non-military vehicle.³⁰ Moreover, the Mine Ban Treaty makes no exceptions for self-destructing or self-deactivating mines,³¹ important exemptions which deny the reality that anti-personnel mines can be used in combat while also mitigating potential harm to civilians. Combined, these two shortfalls have led to a relatively low adoption rate, with only 164 state parties to the Treaty, a number not embracing any of the major cyber warfare powers.³²

²⁹ See Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, art. 2, Sept. 18, 1997, 2056 U.N.T.S. 211 (“Mines designed to be detonated by the presence, proximity or contact of a vehicle as opposed to a person . . . are not considered anti-personnel mines.”); see also *Landmines*, U.N. OFF. FOR DISARMAMENT AFF., <https://www.un.org/disarmament/convarms/landmines>.

³⁰ *Landmines*, *supra* note 29 (discussing the need to regulate anti-vehicle mines as they “continue to cause many casualties, often civilian,” nearly every day around the world).

³¹ See Padraic Convery, *The Ottawa Convention is a Minefield in Itself*, INDEPENDENT (Aug. 30, 1998), <https://www.independent.co.uk/voices/the-ottawa-convention-is-a-minefield-in-itself-1175102.html>.

³² See generally *The Ottawa Convention at a Glance*, ARMS CONTROL ASS’N, <https://www.armscontrol.org/factsheets/ottawa> (last updated Jan. 4, 2018) (“There are 34 non-signatories, including major powers such as the United States, Russia, and China.”).

The fatal flaw of the Mine Ban Treaty was the manner in which it was created. Rather than being the result of intensive, state-on-state diplomacy among the most powerful or involved nations in the matter, the Treaty was spearheaded by non-governmental organizations and second-tier state powers such as Canada, Norway, Austria, and South Africa. As a result, the most powerful nations in the world employing the use of land mines to meet acute security needs by responsible means (e.g., South Korea) have never acceded to the Treaty.³³ In this way, the Treaty makes a practical defense measure the enemy of the good. States also use cluster munitions in a similar fashion and, accordingly, the Convention on Cluster Munitions (CCM)³⁴ has proven to be as unpopular and ineffective as the Mine Ban Treaty.³⁵

E. The Convention on Certain Conventional Weapons

The United States and many other nations are a parties to the Convention on Certain Conventional Weapons (CCW), a treaty prohibiting certain types of conventional weapons known to cause “inhumane injuries” to both combatants and non-combatants alike.³⁶ Additional protocols were passed under the CCW, such as the prohibition against weapons designed to produce medically undetectable shrapnel.³⁷ The CCW places restrictions on landmines,

³³ See generally David Alexander, *U.S. Says Will Abide by Mine Ban Treaty Except on Korean Peninsula*, REUTERS (Sept. 23, 2014), <https://www.reuters.com/article/us-usa-defense-landmines-idUSKCN0HI1U920140923> (noting “the United States sought an exception for Korea during negotiations on the treaty in 1997” but was rebuffed by allies).

³⁴ Convention on Cluster Munitions, Dec. 3, 2008, 2688 U.N.T.S. 39.

³⁵ See generally Jeff Abramson, *Treaty Analysis: The Convention on Cluster Munitions*, ARMS CONTROL TODAY (Dec. 4, 2008), https://www.armscontrol.org/act/2008_12/CCM (indicating countries “holding the majority of the world’s cluster munitions stockpiles” have “thus far not backed the” Convention on Cluster Munitions).

³⁶ Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Apr. 10, 1972, 1342 U.N.T.S. 137; see Jeff Abramson, *Convention on Certain Conventional Weapons (CCW) at a Glance*, ARMS CONTROL ASS’N, <https://www.armscontrol.org/factsheets/CCW> (last updated Sept. 5, 2017).

³⁷ Protocol on Non-Detectable Fragments (Protocol I), Oct. 10, 1980, 1342 U.N.T.S. 168.

incendiary weapons, and blinding lasers, in addition to also establishing guidelines for the removal of unexploded ordnance following the cessation of hostilities.³⁸ New protocols are regularly considered, though the timeline for adoption can be lengthy due to the need to build a consensus among the many signatories. Currently before the body are issues such as small-caliber bullets, anti-vehicle mines, and cluster munitions.³⁹

Paradoxically, passage of a separate, non-CCW sanctioned cluster munition treaty makes the passage of incremental cluster munitions controls harder, not easier. Incremental reform might be possible within the CCW, but an outright ban is not feasible in the near-term. Many nations find cluster munitions essential to their national defense.⁴⁰ States that have agreed to a cluster munitions ban now cannot agree to a lesser, incremental approach within the confines of the CCW when they have already agreed to an outright ban, at least without incurring a high political price.

While the anti-mine and cluster munitions treaties are more targeted than the broad-brushstroke approach of the chemical, biological, and nuclear agreements, they were inherently flawed in their conception and execution. As a result, these treaties potentially have done more harm than good in the long term.

II. NASCENT ATTEMPTS AT CYBER WARFARE AGREEMENTS

In September 2015, President Xi Jinping of China and President Barack Obama of the United States announced a bilateral agreement to curb non-military industrial cyber espionage. While the agreement coincided with a reduction in the rate of Chinese cyber intrusions, the rate had already been on a steady and steep decline at the time, possibly

³⁸ See Abramson, *supra* note 36.

³⁹ *Id.*

⁴⁰ Steven Groves & Theodore Bromund, *The United States Should Not Join the Convention on Cluster Munitions*, HERITAGE FOUND. (Apr. 28, 2011), <https://www.heritage.org/report/the-united-states-should-not-join-the-convention-cluster-munitions>.

due to economic pressure levied on China by the United States.⁴¹ Alternatively, Chinese cyberattacks may have been reduced to focus on a small number of high-value targets with advanced means versus the large-scale, detectable intrusions of the past. Ironically, following the putative success of the U.S.-China cyber agreement (and despite a pre-existing cyber agreement inked between China and Russia) Chinese intrusions of Russian firms actually tripled in the immediate aftermath of the U.S.-China agreement.⁴² While bilateral agreements can help jumpstart wider multilateral cooperation, these efforts are still in their early stages and have met with mixed success, and their enduring nature is yet to be seen.

In 2015, the United Nations published the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE report).⁴³ At just over a dozen pages, what the GGE report lacks in depth and substance is compensated for in its international composition and consensus. The GGE included representatives from twenty countries, and a collection of nations as diverse as Belarus, Brazil, China, Ghana, Israel, Russia, and the United States all participating.

NATO's Cooperative Cyber Defence Centre of Excellence recently updated its extensive *Tallinn Manual on the International Law Applicable to Cyber Warfare*.⁴⁴ The updated manual exhaustively lays out the concordance and dissonance of the existing international law and current cyber practices.⁴⁵ In it, a multitude of distinguished

⁴¹ FIREEYE iSIGHT INTELLIGENCE, RED LINE DRAWN: CHINE RECALCULATES ITS USE OF CYBER ESPIONAGE 3 (2016), <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>.

⁴² Stepan Kravchenko, *Russia More Prey than Predator to Cyber Firm Wary of China*, BLOOMBERG: TECH (Aug. 26, 2016, 5:01 PM), <https://www.bloomberg.com/news/articles/2016-08-25/russia-more-prey-than-predator-to-cyber-firm-wary-of-china>.

⁴³ Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

⁴⁴ TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013); see TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017).

⁴⁵ See TALLINN MANUAL 2.0, *supra* note 44.

scholars and experts from a variety of disciplines present a nuanced reconciliation of extant international law with “this ‘new’ form of warfare.”⁴⁶ The authors address topics as varied as blockades, self-defense, and state responsibility, detailing ninety-five rules where international law and cyber warfare operations intersect. However, these rules are philosophical, not codified, nor agreed upon internationally. They are not perfect, and do not (and likely could not) contain every possible cyber scenario. But projects such as the *Tallinn Manual* provide the perfect starting point for a global dialogue on the parameters of acceptable conduct with regard to international cyber warfare.

China, Russia, and several central Asian nations have alternatively proposed a brief, four-page “International Code of Conduct for Information Security.”⁴⁷ Short on specifics, the Code has been interpreted as advancing the authoritarian principles prevalent in those nations to the detriment of human rights.⁴⁸ While the Code may not as palatable as the *Tallinn Manual*, it shows a shared willingness on the part of many nations to move towards a rationalized international cyber warfare treaty regime, and the potential for a mutually acceptable middle ground between these two approaches exists.

III. RECOMMENDATION

As with any treaty, certain actors will seek to test (or outright violate) the boundaries of agreed-upon civilized behavior. Cyber agreements are complicated by the difficulty in definitive attribution or potential danger of exposing “sources and methods” of purported nation-state cyberattacks. However, if reasonable ground rules could be agreed upon, states-parties would find it in their best interests to abide by a cyber warfare agreement for their own domestic benefits.

⁴⁶ *Id.* at 1.

⁴⁷ See Annex to the Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723, (Jan. 13, 2015).

⁴⁸ Alex Grigsby, *Will China and Russia’s Updated Code of Conduct Get More Traction in a Post-Snowden Era?*, COUNCIL ON FOREIGN REL. (Jan. 28, 2015), <https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era>.

Until such an agreement is crafted and in force, total anarchy will continue to reign.

While it would be infeasible to completely ban cyber weapons as a single class due to the wide range of potentially applicable cyber technology, which includes relatively benign instruments, a targeted approach proscribing the employment of specific cyber weapons would likely be more efficacious. Even so, any targeted approach style agreement would have to avoid the missteps taken by the weapons-specific treaties.

On August 6, 1945, the United States deployed its first atomic bomb in combat in the Japanese city of Hiroshima. Biological weapons have never been employed offensively. Land mines and cluster munitions have been a scourge for decades and still endanger the lives of millions across the world on a daily basis. Thus, international treaties and conventions are evidently only as good as the multinational will which upholds them.

Cyber weapons are not particularly analogous to chemical, biological, or nuclear weapons individually, but they clearly share certain commonalities with all three. Within that context, the treaties governing those weapons are worth considering because they could provide a guidepost for what may or may not work in actual practice. The vague, blanketed prohibitions of the BWC are impracticable for cyber weapons. Globally, there is no consensus on humanitarian rights or norms in the cyber realm, but the lack of a verification mechanism in the BWC is well suited for the cyber environment. Similarly, the proscriptive listing of chemicals in the CWC is a helpful guide, not with regard to specific bits of code, but insofar as evidencing the benefits of promulgating an definitive, unambiguous list of do's and don'ts. Likewise, the NPT provides a cautionary tale, as its core commandment to denuclearize rings hollow in juxtaposition with the reality of nuclear-armed signatories unwilling to forego their key weapons. In retrospect, a treaty placing explicit limits on nuclear weapons might have been a wiser choice than the idealistic and unrealistic goal of attaining global nuclear-zero.

The weapons-specific treaties are further evidence of idealism interfering with execution. Meaningful attempts to curb cyber conduct can only occur with—not without—the involvement of key international players. NATO's *Tallinn Manual* has provided the vast bulk of intellectual legwork necessary to reconcile existing

international law with current cyber warfare. The manual not only provides rules, but also clarifies the gaps and seams that any successor treaty would need to mend. Meanwhile, the United Nations' GGE report provides basis for achieving international consensus, with all of the key cyber actors (except for North Korea) participating in the original United Nations-sanctioned forum. Only four of the twenty nations on the GGE panel—Egypt, Ghana, Kenya, and Malaysia—are not parties to the Convention on Certain Conventional Weapons. As a result, the CCW might be an ideal place start and a fitting mechanism to consider when enacting limits on cyber warfare.

Despite its generic name, the CCW's prohibitions include lasers and other unconventional weapons. But the treaty lacks verification mechanisms, which would be insufficient and infeasible within the cyber context anyway. Still, enacting a new treaty from whole cloth would be far more difficult than proposing an additional protocol to which existing signatories could accede. Although a vague, principles-based approach to curbing cyber warfare is untenable, a clear prohibition of certain acts might be achievable for inclusion into a future CCW protocol. Despite the non-binding nature of the protocols, meaningful pressure could be brought from within the treaty itself to keep rogue signatories in check. Additionally, the inclusion of a cyber protocol in the CCW could also have salutary second-order effects. Any nations that are currently not CCW state-parties might join in order to gain cyber protections and, at the same time, consider other important, non-cyber protocols.

In the coming decades, it is highly probable that bilateral and multilateral agreements will be inked in order to curtail certain deleterious cyber actions. Those cyber actions causing direct tangible harm on widespread civilian populations are likely to be highest on the list of prohibitions. Cyber warfare that enables espionage, tactical or operational battlefield victories, and strategic military or industrial-based sabotage are likely to not be included. Ultimately, the addition of a Cyber Protocol to the Convention is an important first step and a potential mechanism to enact a general international will.

JOURNAL OF LAW & CYBER WARFARE

VOLUME 7

FALL 2018

ISSUE 1

About the Journal

The Journal of Law and Cyber Warfare is published twice per year by top legal professionals and scholars from the law, technology, security, and business industries.

The views expressed in the Journal of Law and Cyber Warfare are those of the authors and not necessarily of the Journal of Law and Cyber Warfare or Lexeprint Inc., the publishing company.

Submissions

The Journal welcomes submissions from legal scholars, technologists, mathematicians, analysts, academics, policy makers, practitioners, lawyers, judges and social scientists. Electronic submissions are encouraged. Submissions by email should be directed to submissions@jlcw.org.

Form

Please cite as: 7 J.L. & CYBER WARFARE ____ (2018).

Copyright

All articles © 2012–2018 by the Journal of Law and Cyber Warfare, except where otherwise expressly indicated. For all articles copyrighted, the Journal permits copies to be made for classroom use, provided that

- (1) the author and the Journal of Law and Cyber Warfare are identified,
- (2) the proper notice of copyright is affixed to each copy,
- (3) each copy is distributed at or below cost, and
- (4) the Journal of Law and Cyber Warfare is notified of the use.

Subscriptions

The cost of an annual subscription is \$250.
Subscription requests should be sent to info@jlcw.org.

Visit us at www.jlcw.org.
